PARA MAC

Guia do Usuário

(destinado ao produto versão 6.0 e posterior)

Clique aqui para fazer o download da versão mais recente deste documento

Atendimento ao cliente: www.eset.com/support

REV. 25. 8. 2015

Índice

1. ESET Endpoint Antivirus

O ESET Endpoint Antivirus 6 representa uma nova abordagem para a segurança do computador verdadeiramente integrada. A versão mais recente do mecanismo de rastreamento ThreatSense® utiliza velocidade e precisão para manter a segurança do seu computador. O resultado é um sistema inteligente que está constantemente em alerta contra ataques e programas maliciosos que podem comprometer seu computador.

O ESET Endpoint Antivirus 6 é uma solução de segurança completa produzida a partir do nosso esforço de longo prazo para combinar proteção máxima e impacto mínimo no sistema. As tecnologias avançadas, com base em inteligência artificial, são capazes de eliminar proativamente a infiltração por vírus, spywares, cavalos de troia, worms, adwares, rootkits e outros ataques via Internet sem prejudicar o desempenho do sistema ou interromper a atividade do computador.

O ESET Endpoint Antivirus 6 foi projetado principalmente para o uso em estações de trabalho em um ambiente de negócios/empresarial. É possível usá-lo com o ESET Remote Administrator 6, permitindo gerenciar facilmente qualquer número de estações de trabalho do cliente, aplicar políticas e regras, monitorar detecções e administrar alterações remotamente a partir de qualquer computador em rede.

1.1 Novidades da versão 6

A interface gráfica do usuário do ESET Endpoint Antivirus foi totalmente reformulada para fornecer melhor visibilidade e uma experiência mais intuitiva para o usuário. Algumas das muitas melhorias incluídas na versão 6 incluem:

- **Proteção do acesso à Web** - monitora a comunicação entre os navegadores da Internet e os servidores remotos
- **Proteção de email** - fornece controle da comunicação por email recebida pelos protocolos POP3 e IMAP
- **Proteção antiphishing** - outra camada de proteção que fornece um nível superior de defesa de sites ilegítimos que tentam adquirir senhas e outras informações confidenciais
- **Controle de dispositivo** - permite rastrear, bloquear ou ajustar filtros/permissões estendidos e define a capacidade de um usuário de acessar e trabalhar com dispositivos externos. Este recurso está disponível na versão 6.1 e posterior do produto.
- **Modo de apresentação** - permite executar o ESET Endpoint Antivirus em segundo plano e suprime janelas pop-up e tarefas agendadas
- **Cache local compartilhado** - permite melhorias na velocidade de rastreamento em ambientes virtualizados

1.2 Requisitos do sistema

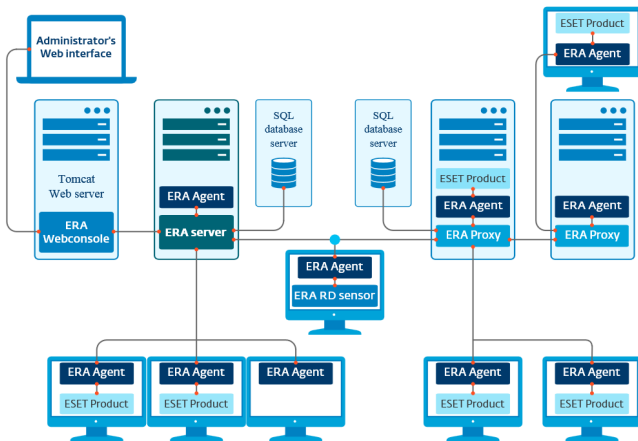
Para uma operação ideal do ESET Endpoint Antivirus, seu sistema deve atender aos seguintes requisitos de hardware e de software:

	Requisitos do sistema:
Arquitetura do processador	Intel 32-bit, 64-bit
Sistema operacional	Mac OS X 10.6 e versões posteriores Mac OS X Server 10.7 e versões posteriores **OBSERVAÇÃO:** Clientes executando o Mac OS X 10.6 não podem ser gerenciados usando o ESET Remote Administrator 6.x
Memória	300 MB
Espaço livre em disco	200 MB

2. Usuários que se conectam via ESET Remote Administrator

ESET Remote Administrator (ERA) 6 é um aplicativo que permite que você gerencie produtos ESET em um ambiente em rede a partir de um local central. O sistema de gerenciamento de tarefas do ESET Remote Administrator permite que você instale soluções de segurança da ESET em computadores remotos e responda rapidamente a novos problemas e ameaças. O ESET Remote Administrator não fornece proteção contra código malicioso por si só, ele conta com a presença de uma solução de segurança da ESET em cada cliente.

As soluções de segurança da ESET são compatíveis com redes que incluem vários tipos de plataforma. Sua rede pode incluir uma combinação de sistemas operacionais Microsoft, Linux e OS X que são executados em dispositivos móveis (celulares e tablets).

A imagem a seguir mostra uma arquitetura de exemplo para uma rede protegida por soluções de segurança da ESET gerenciada por ERA:

OBSERVAÇÃO: Para mais informações consulte a ESET Remote Administrator documentação online.

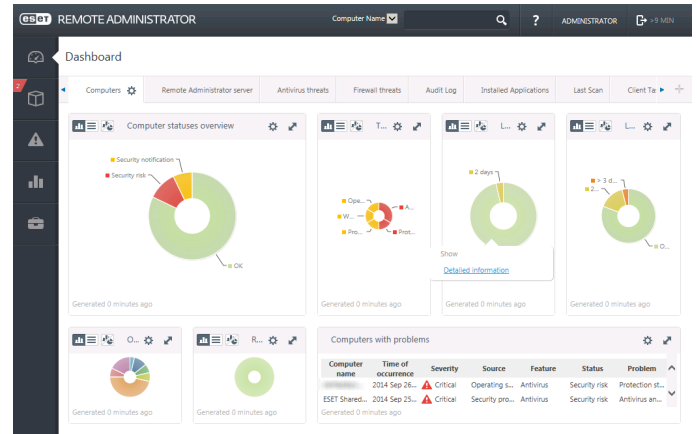
2.1 Servidor do ESET Remote Administrator

Servidor do ESET Remote Administrator é o componente executivo do ESET Remote Administrator. Ele processa todos os dados recebidos de clientes que se conectam ao Servidor (por meio do Agente ERA 6). O Agente ERA facilita a comunicação entre o cliente e o servidor. Dados (relatórios de cliente, configuração, replicação do agente, etc.) são armazenados em um banco de dados que o ERA acessa para fornecer relatórios.

Para processar dados corretamente, o Servidor ERA exige uma conexão estável com um servidor de banco de dados. Recomendamos que você instale o Servidor ERA e seu banco de dados em servidores separados para otimizar o desempenho. A máquina na qual o Servidor ERA está instalado deve ser configurada para aceitar todas as conexões de Agente/Proxy/RD Sensor, que são verificadas usando certificados. Uma vez que o Servidor ERA está instalado, é possível abrir o Console da Web ERA 5 que permite gerenciar as estações de trabalho do endpoint com soluções ESET instaladas.

2.2 Console da Web

O **ERA console da Web** é uma interface de usuário na Web que apresenta dados do Servidor ERA 5 e permite que você gerencie as soluções de segurança da ESET em seu ambiente. O Console da Web pode ser acessado usando um navegador. Ele exibe uma visão geral do status de clientes em sua rede e pode ser usado para implantar remotamente soluções da ESET em computadores não gerenciados. Você pode escolher tornar o servidor Web acessível pela internet, para permitir o uso do ESET Remote Administrator de praticamente qualquer lugar ou dispositivo.

O Painel do Console da Web:

A ferramenta **Pesquisa rápida** está localizada na parte superior do console da Web. Selecione **Nome do computador**, **Endereço IPv4/IPv6** ou **Nome da ameaça** no menu suspenso, digite sua sequência de pesquisa no campo de texto e clique no símbolo da lente de aumento ou pressione **Enter** para pesquisar. Você será redirecionado para a seção Grupos, onde seu resultado de pesquisa será exibido.

2.3 Proxy

Proxy ERA é outro componente do ESET Remote Administrator com duas finalidades principais. No caso de uma rede de médio porte ou corporativa com muitos clientes (por exemplo, 10.000 clientes ou mais), você pode usar o Proxy ERA para distribuir a carga entre vários Proxies ERA, facilitando para o Servidor ERA 5 principal. A outra vantagem do Proxy ERA é que você pode usá-lo ao se conectar a uma filial remota com um link fraco. Isso significa que o Agente ERA em cada cliente não está conectando ao Servidor ERA principal diretamente através do Proxy ERA, que está na mesma rede local da filial. Esta configuração libera o link da filial. O Proxy ERA aceita conexões de todos os Agentes ERA locais, compila seus dados e os envia para o Servidor ERA principal (ou outro Proxy ERA). Isso permite que sua rede acomode mais clientes sem comprometer o desempenho de suas consultas de banco de dados e rede.

Dependendo da configuração de sua rede, é possível que um Proxy ERA se conecte a outro Proxy ERA e então se conecte ao Servidor ERA principal.

Para o funcionamento correto do Proxy ERA, o computador host no qual você instalará o Proxy ERA deverá ter um Agente da ESET instalado e deve estar conectado ao nível superior (seja Servidor ERA ou Proxy ERA superior, se houver um) de sua rede.

2.4 Agente

O **Agente ERA** é uma parte essencial do produto ESET Remote Administrator. As soluções de segurança ESET nas máquinas dos clientes (por exemplo ESET Endpoint Antivirus) comunicam-se com o Servidor ERA exclusivamente por meio do Agente. Esta comunicação permite o gerenciamento das soluções de segurança ESET em todos os clientes remotos a partir de um local central. O Agente coleta informações do cliente e as envia para o Servidor. Quando o Servidor envia uma tarefa para o cliente, ela é enviada para o Agente, que então comunica-se com o cliente. Toda a comunicação em rede ocorre entre o Agente e a parte superior da rede do ERA: Servidor e Proxy.

O Agente ESET usa um dos seguintes três métodos para se conectar ao Servidor:

1. O Agente do Cliente é diretamente conectado ao Servidor.
2. O Agente do Cliente se conecta através de um Proxy, que é conectado ao Servidor.
3. O Agente do Cliente é conectado ao Servidor através de vários Proxies.

O Agente ESET comunica-se com soluções da ESET instaladas em um cliente, coleta informações de programas nesse cliente e transmite as informações de configuração recebidas do Servidor para o cliente.

OBSERVAÇÃO: o proxy da ESET tem seu próprio Agente, que processa todas as tarefas de comunicação entre clientes, outros proxies e o Servidor.

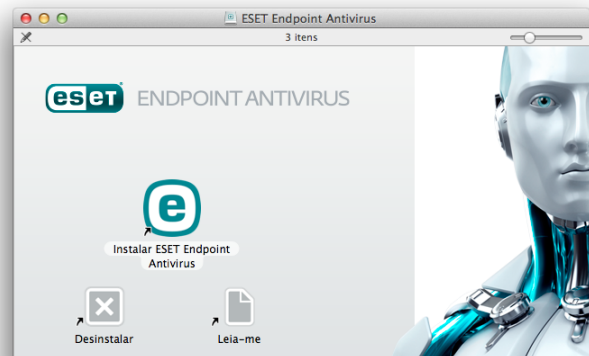
2.5 Sensor RD

Sensor RD (Rogue Detection) é parte do ESET Remote Administrator desenvolvido para encontrar computadores na sua rede. Ele oferece uma forma conveniente de adicionar novos computadores ao ESET Remote Administrator sem a necessidade de encontrá-los e adicioná-los manualmente. Todo computador detectado em sua rede é exibido no console da Web e é adicionado por padrão ao grupo Todos. A partir daí, é possível realizar ações adicionais com computadores cliente individuais.

O RD Sensor consiste em um mecanismo de escuta passivo que detecta computadores que estão presentes na rede e envia informações sobre eles para o Servidor ERA. O Servidor ERA avalia se os PCs detectados na rede são desconhecidos ou se já são gerenciados.

3. Instalação

Há duas maneiras de iniciar o ESET Endpoint Antivirus para o instalador Mac:

- Se você estiver instalando a partir do CD/DVD de instalação, insira o disco no drive de CD/DVD-ROM e clique duas vezes no ícone de instalação ESET Endpoint Antivirus para iniciar o instalador.
- Se estiver instalando a partir de um arquivo obtido por download, clique duas vezes no arquivo que obteve por download para iniciar o instalador.

O assistente de instalação o guiará pela configuração básica. Durante a fase inicial da instalação, o instalador verificará automaticamente on-line se há uma versão mais recente do produto. Se uma versão mais recente for encontrada, você receberá a opção de baixar a versão mais recente antes de continuar o processo de instalação.

Após concordar com o Contrato de licença de usuário final, você poderá escolher um dos seguintes tipos de instalação:

- Instalação típica 6
- Instalação personalizada 7
- Instalação remota 8

3.1 Instalação típica

O modo de instalação típica inclui opções de configuração apropriadas para a maioria dos usuários. Essas configurações proporcionam segurança máxima combinada com o excelente desempenho do sistema. A instalação típica é a opção padrão e é recomendada se você não tiver requisitos particulares para configurações específicas.

ESET Live Grid
O ESET Live Grid Early Warning System ajuda a assegurar que a ESET seja informada contínua e imediatamente sobre novas infiltrações para proteger rapidamente seus clientes. O sistema permite o envio de novas ameaças para o Laboratório de ameaças da ESET, onde elas serão analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Clique em **Configurar** para modificar as configurações detalhadas sobre o envio de arquivos suspeitos. Para obter mais informações, consulte Live Grid 24.

Aplicativos potencialmente indesejados
A última etapa do processo de instalação é a configuração da detecção de **Aplicativos potencialmente indesejados**. Esses programas não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento.

Após instalar o ESET Endpoint Antivirus, você deve executar um rastreamento do computador para verificar se há código malicioso. Na janela principal do programa, clique em **Rastreamento do computador** e depois em **Rastreamento inteligente**. Para obter mais informações sobre rastreamentos sob demanda do computador, consulte a seção Rastreamento sob demanda do computador 13.

3.2 Instalação personalizada

O modo de instalação personalizada é destinado a usuários experientes que desejam modificar configurações avançadas durante o processo de instalação.

Componentes do programa
O ESET Endpoint Antivirus permite que você instale o produto sem alguns de seus componentes centrais (por exemplo, Proteção web e email). Desmarque a caixa de seleção ao lado de um componente de produto para removê-lo da instalação.

Servidor proxy
Se estiver usando um servidor proxy, é possível definir seus parâmetros selecionando **Eu utilizo um servidor proxy**. Na próxima janela, digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. No campo Porta, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Se o servidor proxy exigir autenticação, digite um **Nome de usuário** e uma **Senha** válidos para obter acesso ao servidor proxy. Se você não utilizar um servidor proxy, selecione **Eu não utilizo um servidor proxy**. Se você não tem certeza se usa um servidor proxy ou não, é possível usar suas configurações atuais do sistema selecionando **Usar configurações do sistema (recomendado)**.

Privilégios
Na próxima etapa, você poderá definir usuários ou grupos privilegiados que poderão editar a configuração do programa. A partir da lista de usuários na esquerda, selecione os usuários e **Adicione** na lista de **Usuários privilegiados**. Para mostrar todos os usuários do sistema, selecione **Mostrar todos os usuários**. Se você deixar a lista Usuários privilegiados vazia, todos os usuários serão considerados privilegiados.

ESET Live Grid
O ESET Live Grid Early Warning System ajuda a assegurar que a ESET seja informada contínua e imediatamente sobre novas infiltrações para proteger rapidamente seus clientes. O sistema permite o envio de novas ameaças para o Laboratório de ameaças da ESET, onde elas serão analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Clique em **Configurar...** para modificar as configurações detalhadas sobre o envio de arquivos suspeitos. Para obter mais informações, consulte Live Grid 24.

Aplicativos potencialmente indesejados
A próxima etapa do processo de instalação é a configuração da detecção de **Aplicativos potencialmente indesejados**. Esses programas não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento.

Após instalar o ESET Endpoint Antivirus, você deve executar um rastreamento do computador para verificar se há código malicioso. Na janela principal do programa, clique em **Rastreamento do computador** e depois em **Rastreamento inteligente**. Para obter mais informações sobre rastreamentos sob demanda do computador, consulte Rastreamento sob demanda do computador 13.

3.3 Instalação remota

A instalação remota permite que você crie um pacote de instalação que pode ser instalado em computadores de destino que utilizem software de área de trabalho remota. Quando a instalação estiver concluída, o ESET Endpoint Antivirus pode ser gerenciado remotamente através do ESET Remote Administrator.

A instalação remota é realizada em duas etapas:

1. Criação de um pacote de instalação remota usando o instalador ESET 8
2. Instalação remota utilizando o software de área de trabalho remota 9

Utilizando a versão mais recente do ESET Remote Administrator 6, você também pode executar uma instalação remota em computadores OS X do cliente. Para obter instruções detalhadas siga os passos descritos neste artigo da Base de Conhecimento. (É possível que o artigo não esteja disponível em seu idioma.)

3.3.1 Criação de um pacote de instalação remota

Componentes do programa

O ESET Endpoint Antivirus permite que você instale o produto sem alguns de seus componentes centrais (por exemplo, Proteção web e email). Desmarque a caixa de seleção ao lado de um componente de produto para removê-lo da instalação.

Servidor proxy

Se estiver usando um servidor proxy, é possível definir seus parâmetros selecionando **Eu utilizo um servidor proxy**. Na próxima janela, digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. No campo Porta, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Se o servidor proxy exigir autenticação, digite um **Nome de usuário** e uma **Senha** válidos para obter acesso ao servidor proxy. Se você não utilizar um servidor proxy, selecione **Eu não utilizo um servidor proxy**. Se você não tem certeza se usa um servidor proxy ou não, é possível usar suas configurações atuais do sistema selecionando **Usar configurações do sistema (recomendado)**.

Privilégios

Na próxima etapa, você poderá definir usuários ou grupos privilegiados que poderão editar a configuração do programa. A partir da lista de usuários na esquerda, selecione os usuários e **Adicione** na lista de **Usuários privilegiados**. Para mostrar todos os usuários do sistema, selecione **Mostrar todos os usuários**. Se você deixar a lista Usuários privilegiados vazia, todos os usuários serão considerados privilegiados.

ESET Live Grid

O ESET Live Grid Early Warning System ajuda a assegurar que a ESET seja informada contínua e imediatamente sobre novas infiltrações para proteger rapidamente seus clientes. O sistema permite o envio de novas ameaças para o Laboratório de ameaças da ESET, onde elas serão analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Clique em **Configurar...** para modificar as configurações detalhadas sobre o envio de arquivos suspeitos. Para obter mais informações, consulte Live Grid 24.

Aplicativos potencialmente indesejados

A próxima etapa do processo de instalação é a configuração da detecção de **Aplicativos potencialmente indesejados**. Esses programas não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento.

Arquivos de instalação remota

Na última etapa do assistente de instalação, selecione uma pasta de destino para o pacote de instalação (*esets_remote_Install.pkg*), o script do shell de instalação (*esets_setup.sh*) e o script do shell de desinstalação (*esets_remote_UnInstall.sh*).

3.3.2 Instalação remota em computadores de destino

O ESET Endpoint Antivirus pode ser instalado nos computadores de destino usando o Apple Remote Desktop ou qualquer outra ferramenta compatível com a instalação de pacotes Mac padrão (*.pkg*), ao copiar os arquivos e executar scripts shell nos computadores de destino.

Para instalar o ESET Endpoint Antivirus usando o Apple remote desktop:

1. Clique em **Copiar** no Apple remote desktop.
2. Clique em **+**, vá até o script shell de instalação *(esets_setup.sh)* e selecione.
3. Selecione **/tmp** do manu suspenso **Colocar itens em** e clique em **Copiar**.
4. Clique em **Instalar** para enviar o pacote para seus computadores de destino.

Para obter instruções detalhadas sobre como administrar computadores cliente usando o ESET Remote Administrator, consulte a ESET Remote Administrator documentação on-line.

3.3.3 Desinstalação remota

Para desinstalar o ESET Endpoint Antivirus de computadores clientes:

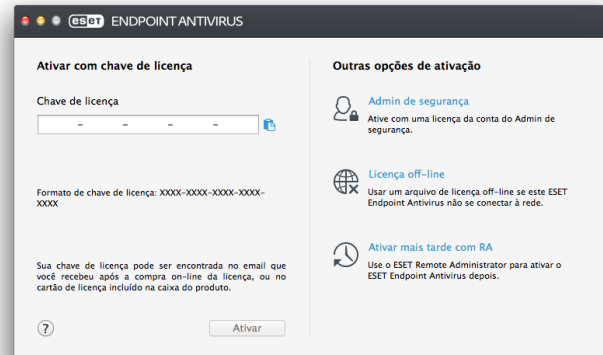
1. Usando o comando **Copiar itens** no Apple Remote Desktop, localize o script shell de desinstalação (*esets_remote_unInstall.sh* - criado junto com o pacote de instalação) e copie o script shell para o diretório /tmp em computadores de destino (por exemplo, */tmp/esets_remote_uninstall.sh*).
2. Selecione o Usuário sob **Executar comando como** e digite **root** no campo **Usuário**.
3. Clique em **Enviar**. Após a instalação bem sucedida, um registro de console será exibido.

3.3.4 Atualização remota

Use o comando **Instalar pacotes** no Apple Remote Desktop para instalar a versão mais recente do ESET Endpoint Antivirus quando uma nova versão estiver disponível.

4. Ativação do produto

Após a conclusão da instalação, você será solicitado a ativar o produto. Existem vários métodos de ativação que podem ser usados. A disponibilidade de um método específico de ativação pode variar conforme o país, assim como os meios de distribuição (CD/DVD, página da web da ESET, etc.) para seu produto.

Para ativar sua cópia do ESET Endpoint Antivirus diretamente do programa, clique no ícone ESET Endpoint Antivirus localizado na barra de menu OS X (parte superior da tela) e clique em **Ativação do produto**. Também é possível ativar seu produto no menu principal em **Ajuda** > **Gerenciar licenças** ou **Status da proteção** > **Ativar produto**.

Você pode usar qualquer um dos seguintes métodos para ativar o ESET Endpoint Antivirus:

- **Chave de licença** - Uma sequência exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX, que é usado para identificação do proprietário da licença e para ativação da licença. Sua chave de licença pode ser encontrada no email que você recebeu após a compra da licença, ou no cartão de licença incluído na caixa.
- **Admin de segurança** - Uma conta criada no portal do ESET License Administrator com credenciais (endereço de email e senha). Esse método permite que você gerencie várias licenças de um local.
- **Licença offline** - Um arquivo gerado automaticamente que será transferido para o produto da ESET para fornecer informações de licença. Seu arquivo de licença off-line é gerado do portal do ESET License Administrator e é usado em ambientes nos quais o aplicativo não pode se conectar à autoridade de licenciamento.

Clique em **Ativar mais tarde com RA** se seu computador for um membro da rede gerenciada e seu administrador planejar usar o ESET Remote Administrator para ativar seu produto. Você também pode usar esta opção se quiser ativar este cliente em posteriormente.

OBSERVAÇÃO: ESET Remote Administrator é capaz de ativar computadores cliente em segundo plano usando licenças disponibilizadas pelo administrador.

5. Desinstalação

Há várias maneiras de iniciar o ESET Endpoint Antivirus para o desinstalador Mac:

- insira o CD/DVD de instalação do ESET Endpoint Antivirus em seu computador, abra-o a partir de sua área de trabalho ou na janela **Finder** e clique duas vezes em **Desinstalar**
- abra o arquivo de instalação ESET Endpoint Antivirus (*.dmg*) e clique duas vezes em **Desinstalar**
- inicie o **Finder**, abra a pasta **Aplicativos** no seu disco rígido, segure a tecla CTRL e clique no ícone **ESET Endpoint Antivirus** e selecione **Mostrar conteúdo do pacote**. Abra a pasta **Contents** > **Helpers** e dê um clique duplo no ícone **Uninstaller**.

6. Visão geral básica

A janela principal do ESET Endpoint Antivirus é dividida em duas seções principais. A primeira janela à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

As seções a seguir são acessíveis a partir do menu principal:

- **Status da proteção** - fornece informações sobre o status da proteção de sua proteção de email, web e computador.
- **Rastrear o computador** - esta seção permite configurar e iniciar o Rastreamento sob demanda do computador 13.
- **Atualizar** - exibe informações sobre as atualizações do banco de dados de assinatura de vírus.
- **Configuração** - selecione esta seção para ajustar o nível de segurança do seu computador.
- **Ferramentas** - Fornece acesso a Relatórios 21, Agenda 23, Quarentena 25, Processos em execução 27 e outros recursos do programa.
- **Ajuda** - exibe acesso a arquivos de ajuda, base de dados de conhecimento da Internet, formulário de solicitação de suporte e informações adicionais sobre o programa.

6.1 Atalhos do teclado

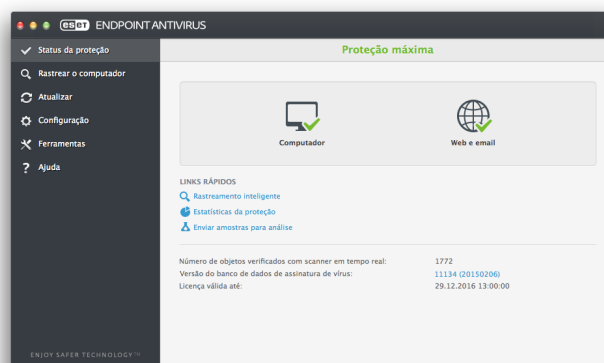
As teclas de atalho que podem ser usadas ao trabalhar com o ESET Endpoint Antivirus incluem:

- *cmd+,* - exibe as preferências do ESET Endpoint Antivirus,
- *cmd+O* - redimensiona a janela de interface gráfica do usuário principal do ESET Endpoint Antivirus para o tamanho padrão e a move para o centro da tela,
- *cmd+Q* - esconde a janela principal da interface gráfica do usuário do ESET Endpoint Antivirus. Você pode abri-lo clicando no ícone ESET Endpoint Antivirus na barra de menus do OS X (parte superior da tela),
- *cmd+W* - fecha a janela principal da interface gráfica do usuário do ESET Endpoint Antivirus.

Os seguintes atalhos de teclado funcionam apenas se **Usar menu padrão** estiver ativado em **Configuração** > **Entrar nas preferências do aplicativo...** > **Interface**:

- *cmd+alt+L* - abre a seção de **Relatórios**,
- *cmd+alt+S* - abre a seção da **Agenda**,
- *cmd+alt+Q* - abre a seção de **Quarentena**.

6.2 Verificação do funcionamento do sistema

Para visualizar seu status de proteção, clique em **Status de proteção** no menu principal. Um resumo de status sobre o funcionamento dos módulos do ESET Endpoint Antivirus será exibido na janela principal.

6.3 O que fazer se o programa não funcionar adequadamente

Quando um módulo está funcionando corretamente, um ícone de marca de verificação verde é exibido. Quando um módulo não está funcionando corretamente, um ponto de exclamação vermelho ou um ícone de notificação laranja é exibido. Informações adicionais sobre o módulo e uma proposta de solução para corrigir o problema são exibidos na janela principal do programa. Para alterar o status dos

módulos individuais, clique no link azul abaixo de cada mensagem de notificação.

Se não for possível resolver um problema com as soluções sugeridas, você pode procurar na Base de conhecimento ESET para uma solução ou entrar em contato com o Atendimento ao Cliente ESET. O Atendimento ao cliente responderá rapidamente às suas perguntas e ajudará a resolver quaisquer problemas com o ESET Endpoint Antivirus.

7. Proteção do computador

A configuração do Computador pode ser encontrada em **Configuração** > **Computador**. Ela exibe o status da **Proteção em tempo real do sistema de arquivos**. Para desativar módulos individuais, alterne o módulo desejado para **DESATIVADO**. Observe que isso pode diminuir o nível de proteção do seu computador. Para acessar as configurações detalhadas para cada módulo, clique em **Configuração**.

7.1 Proteção antivírus e antispyware

A proteção antivírus protege contra ataques de sistemas maliciosos, modificando arquivos que representam ameaças internas. Se uma ameaça com código malicioso for detectada, o módulo antivírus poderá eliminá-la, bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena.

7.1.1 Geral

Na seção **Geral** (**Configuração** > **Entrar nas preferências do aplicativo...** > **Geral**), é possível ativar a detecção dos seguintes tipos de aplicativos:

- **Aplicativos potencialmente indesejados** - Esses aplicativos não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de maneira negativa. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao modo anterior à instalação desses aplicativos). As alterações mais significativas são janelas pop-up indesejadas, ativação e execução de processos ocultos, aumento do uso de recursos do sistema, modificações nos resultados de pesquisa e aplicativos se comunicando com servidores remotos.
- **Aplicativos potencialmente inseguros** - esses aplicativos são softwares comerciais e legítimos que podem sofrer abusos por parte de invasores, caso tenham sido instalados sem o conhecimento do usuário. Essa classificação inclui programas como ferramentas de acesso remoto, motivo pelo qual essa opção, por padrão, é desativada.
- **Aplicativos suspeitos** - esses aplicativos incluem programas compactados com empacotadores ou protetores. Esses tipos de protetores são frequentemente explorados por autores de malware para impedir a detecção. Um Empacotador é um executável de extração automática do tempo de execução que inclui vários tipos de malware em um único pacote. Os empacotadores mais comuns são UPX, PE_Compact, PKLite e ASPack. O mesmo malware pode ser detectado de forma diferente quando compactado usando outro empacotador. Os empacotadores também têm a capacidade de tornar suas "assinaturas" mutáveis ao longo do tempo, tornando mais difícil a detecção e remoção do malware.

Para configurar Sistema de arquivo ou Exclusões de web e email 11, clique em **Configuração**.

7.1.1.1 Exclusões

Na seção **Exclusões** você pode excluir certos arquivos/ pastas, aplicativos ou endereços IP/IPv6 do rastreamento.

Arquivos e pastas relacionados na guia **Sistema de arquivos** serão excluídos de todos os rastreamentos: Inicialização, Tempo Real e Sob demanda (rastreamento do computador).

- **Caminho** - caminho para arquivos e pastas excluídos
- **Ameaça** - se houver um nome de uma ameaça próximo a um arquivo excluído, significa que o arquivo só foi excluído para a determinada ameaça, mas não completamente. Se o arquivo for infectado posteriormente com outro malware, ele será detectado pelo módulo antivírus.
- + - cria uma nova exclusão. Digite o caminho para um objeto (você também pode usar os curingas *e ?) ou selecione a pasta ou arquivo a partir da estrutura da árvore.
- − - remove as entradas selecionadas
- **Padrão** – cancela todas as exclusões

Na guia **Web e email**, você pode excluir determinados **Aplicativos** ou **Endereços IP/IPv6** do rastreamento de protocolos.

7.1.2 Proteção de inicialização

Rastrear arquivos na inicialização rastreia arquivos automaticamente no momento da inicialização do sistema. Por padrão, esse rastreamento é executado regularmente como uma tarefa agendada depois de um logon do usuário ou após uma atualização bem sucedida do banco de dados de vírus. Para modificar as configurações de parâmetros do mecanismo ThreatSense aplicáveis ao rastreamento de inicialização, clique em **Configuração**. Você pode saber mais sobre a Configuração do mecanismo ThreatSense lendo esta seção 15.

7.1.3 Proteção em tempo real do sistema de arquivos

A proteção do sistema de arquivos em tempo real verifica todos os tipos de mídia e aciona um rastreamento com base em vários eventos. Com a utilização da tecnologia ThreatSense (descrita na seção Configuração de parâmetros do mecanismo ThreatSense 15), a proteção em tempo real do sistema de arquivos pode variar para arquivos recém-criados e existentes. Arquivos recém-criados podem ser controlados com mais precisão.

Por padrão, a proteção em tempo real é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outro rastreamento em tempo real), a proteção em tempo real pode ser desativada clicando no ícone ESET Endpoint Antivirus localizado na barra de menu (topo da tela) e selecionando **Desativar a proteção em tempo real do sistema de arquivos**. A proteção em tempo real do sistema de arquivos também pode ser desativada na tela principal do programa (clique em **Configuração** > **Computador** e altere **Proteção em tempo real do sistema de arquivos** para **DESATIVADO**).

Para modificar configurações avançadas para Proteção em tempo real do sistema de arquivos, vá para **Configurações** > **Entrar nas preferências do aplicativo...** (ou pressione *cmd+,*) > **Proteção em tempo real** e clique em **Configurar...** ao lado de **Opções Avançadas** (descritos nas Opções avançadas de rastreamento 12).

7.1.3.1 Rastreamento ativado (Rastreamento disparado por evento)

Por padrão, todos os arquivos são rastreados na abertura, criação ou execução do arquivo. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador.

7.1.3.2 Opções de rastreamento avançadas

Nessa janela, é possível definir os tipos de objeto que serão rastreados pelo mecanismo de rastreamento ThreatSense, e ativar/desativar **Heurística avançada** e também modificar as configurações de arquivos compactados e cache de arquivo.

Não recomendamos alterar os valores padrão na seção **Configurações padrão de arquivos compactados**, a menos que seja necessário resolver um problema específico, pois os valores maiores de compactação de arquivos compactados podem impedir o desempenho do sistema.

Você pode alternar o rastreamento de heurística avançada do ThreatSense para arquivos executados, criados e modificados separadamente, selecionando a caixa de seleção **Heurística avançada** em cada uma das respectivas seções de parâmetros do ThreatSense.

Para minimizar a pegada do sistema ao usar a Proteção em tempo real, você pode definir o tamanho do cache de otimização. O cache de otimização é usado sempre que **Ativar cache de arquivo limpo** estiver habilitado. Se esse recurso for desativado, todos os arquivos serão rastreados toda vez que forem acessados. Os arquivos não serão rastreados repetidamente após serem ocultados (a menos que sejam modificados), até o tamanho definido do cache. Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus.

Clique em **Ativar cache de arquivo limpo** para ativar/ desativar essa função. Para especificar o tamanho do cache, insira o valor desejado no campo de entrada ao lado de **Tamanho de cache**.

Os parâmetros de rastreamento adicionais podem ser configurados na janela **Configuração do mecanismo ThreatSense**. Você pode definir qual tipo de **Objetos** devem ser rastreados usando as **Opções** e nNível de **Limpeza**, e definir as **Extensões** e **Limites** de tamanho de arquivos para a proteção em tempo real do sistema de arquivos. Você pode entrar na janela de configuração do mecanismo do ThreatSense clicando em **Configuração** ao lado do **Mecanismo ThreatSense** na janela de configuração avançada. Para obter informações mais detalhadas sobre os parâmetros do mecanismo ThreatSense, consulte Configuração de parâmetros do mecanismo ThreatSense 15.

7.1.3.3 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Tenha cautela ao modificar os parâmetros da proteção em tempo real. Recomendamos que você modifique esses parâmetros apenas em casos específicos. Por exemplo, se houver uma situação de conflito com um certo aplicativo ou rastreador em tempo real de outro programa antivírus.

Após instalar o ESET Endpoint Antivirus, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique no botão **Padrão** localizado na parte inferior esquerda da janela **Proteção em tempo real** (**Configuração** > **Entrar nas preferências do aplicativo ...** > **Proteção em tempo real**).

7.1.3.4 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, utilize o arquivo de teste eicar.com. Esse arquivo de teste é especial, inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pelo instituto EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus.

Para verificar o status da proteção em tempo real sem usar o ESET Remote Administrator, conecte-se ao computador do cliente remotamente usando o **Terminal** e execute o seguinte comando:

```
/Applications/.esets/Contents/MacOS/esets_daemon
--status
```

O status do Rastreamento em tempo real será exibido como `RTPStatus=Enabled` ou `RTPStatus=Disabled`.

O resultado do ataque ao Terminal inclui os status a seguir:

- a versão do ESET Endpoint Antivirus instalada no computador do cliente
- data e versão do banco de dados de assinatura de vírus
- path ao servidor de atualização

OBSERVAÇÃO: O uso do recurso de Terminal é recomendado apenas para usuários avançados.

7.1.3.5 O que fazer se a proteção em tempo real não funcionar

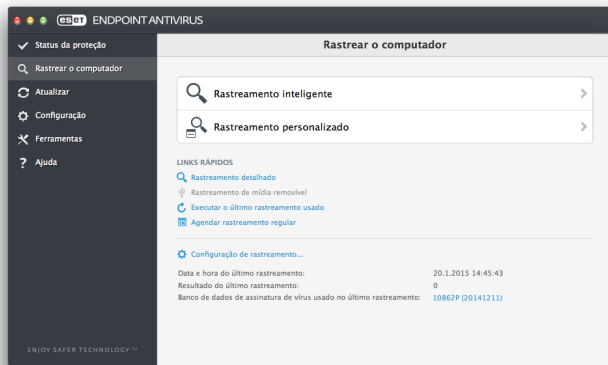
Neste capítulo, descrevemos situações problemáticas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada
Se a proteção em tempo real foi inadvertidamente desativada por um usuário, é preciso reativá-la. Para reativar a Proteção em tempo real, no menu principal clique em **Configuração** > **Computador** e troque **Proteção em tempo real do sistema de arquivos** para **ATIVADO**. Alternativamente, é possível ativar a Proteção em tempo real do sistema de arquivos na janela de preferências de aplicativo em **Proteção em tempo real** selecionando **Ativar a proteção em tempo real do sistema de arquivos**.

Proteção em tempo real não detecta nem limpa infiltrações
Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas podem entrar em conflito. Recomendamos desinstalar outros programas antivírus que possam estar no sistema.

A proteção em tempo real não é iniciada
Se a proteção em tempo real não for ativada na inicialização do sistema, talvez haja conflitos com outros programas. Se isso acontecer, entre em contato com o Atendimento ao Cliente da ESET.

7.1.4 Rastreamento sob demanda do computador

Se você tem suspeitas de que seu computador está infectado (ele se comporta de forma anormal), execute um **Rastreamento inteligente** para examinar seu computador em busca de infiltrações. Para a proteção máxima, rastreamentos do computador devem ser executados regularmente como parte das medidas usuais de segurança, não só quando há suspeita de uma infecção. O rastreamento normal pode detectar infiltrações que não foram detectadas pelo rastreador em tempo real quando foram salvas no disco. Isso pode acontecer caso o rastreador em tempo real esteja desativado no momento da infecção ou se o banco de dados de assinatura de vírus não estiver atualizado.

Recomendamos que execute um Rastreamento sob demanda do computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Agenda**.

Você também pode arrastar e soltar pastas e arquivos da sua área de trabalho ou da janela do **Finder** para a tela principal do ESET Endpoint Antivirus, para o ícone de âncora, ícone da barra de menu (parte superior da tela) ou para o ícone do aplicativo (localizado na pasta */Aplicativos*).

7.1.4.1 Tipos de rastreamento

Há dois tipos de rastreamento sob demanda do computador disponíveis. O **Rastreamento inteligente** rastreia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

7.1.4.1.1 Rastreamento inteligente

O Rastreamento inteligente permite que você inicie rapidamente um rastreamento do computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. Sua principal vantagem é a operação fácil, sem configurações de rastreamento detalhadas. O Rastreamento inteligente verifica todos os arquivos em todas as pastas e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte Limpeza 16.

7.1.4.1.2 Rastreamento personalizado

O **rastreamento personalizado** permite especificar parâmetros de rastreamento, como destinos de rastreamento e métodos de rastreamento. A vantagem de executar um rastreamento personalizado é a capacidade de configurar os parâmetros de rastreamento detalhadamente. Configurações diferentes podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

Para selecionar os destinos de rastreamento, selecione **Rastreamento do computador** > **Rastreamento personalizado** e selecione uma opção no menu suspenso **Destinos de rastreamento** ou selecione destinos específicos na estrutura em árvore. Um destino de rastreamento pode ser também mais exatamente especificado por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração...** > **Limpeza**.

OBSERVAÇÃO: A realização de rastreamentos de computador com o Rastreamento personalizado só é recomendada para usuários avançados com experiência anterior na utilização de programas antivírus.

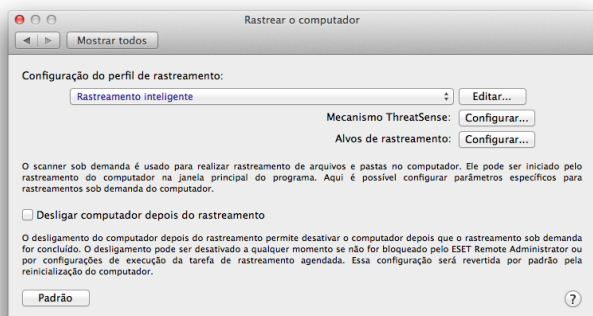
7.1.4.2 Destinos de rastreamento

A estrutura em árvore de Destinos de rastreamento permite que você selecione arquivos e pastas que serão rastreados em busca de vírus. As pastas também podem ser selecionadas de acordo com as configurações de um perfil.

Um destino de rastreamento pode ser mais exatamente especificado por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir no rastreamento. Selecione destinos a partir da estrutura de árvore que lista todas as pastas disponíveis no computador ao selecionar a caixa de seleção correspondente a um determinado arquivo ou pasta.

7.1.4.3 Perfis de rastreamento

As suas configurações de rastreamento favoritas podem ser salvas para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos destinos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, no menu principal clique em **Configuração** > **Entrar nas preferências do aplicativo ...** (ou pressione *cmd+,*) > **Rastreamento do computador** e clique em **Editar** ao lado da lista de perfis atuais.

Para ajudar a criar um perfil de rastreamento a fim de atender às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense 15 para obter uma descrição de cada parâmetro da configuração de rastreamento.

Exemplo: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a Limpeza rigorosa. Na janela **Lista de perfis do rastreamento sob demanda**, digite o nome do perfil, clique em **Adicionar** e confirme clicando em **OK**. Ajuste os demais parâmetros de maneira a atender as suas necessidades usando as configurações **Mecanismo ThreatSense** e **Destinos para rastreamento**.

Se quiser desativar o sistema operacional e desligar o computador depois da conclusão do rastreamento sob demanda, use a opção **Desligar computador depois do rastreamento**.

7.1.5 Configuração de parâmetros do mecanismo ThreatSense

o ThreatSense é uma tecnologia proprietária da ESET composto de vários métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante as primeiras horas da propagação de uma nova ameaça. Ela utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também previne os rootkits com êxito.

As opções de configuração da tecnologia ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados
- A combinação de diversos métodos de detecção
- Níveis de limpeza etc.

Para configurar os parâmetros do mecanismo ThreatSense para os diferentes módulos do produto, clique em **Configuração> Entrar nas preferências do aplicativo** e clique em **Proteção de inicialização**, **Proteção em tempo real** ou **Rastreamento do computador** , dependendo do módulo para o qual você deseja editar as configurações**.** Clique em Configuração ao lado do mecanismo ThreatSense para fazer alterações de configuração específicas para esse módulo do produto. Definições de configuração do ThreatSense são divididas em cinco guias onde você pode configurar os tipos de objetos a serem rastreados, métodos de rastreamento, configurações de limpeza, extensões de arquivos a serem excluídos, limites de tamanho de arquivo ao rastrear e uso da otimização inteligente. Configurações contidas em cada guia são descritas nas seções a seguir. Clique em OK quando terminar de fazer alterações para aplicar as definições no módulo de produto selecionado.

- **Proteção de inicialização** - Rastreamento de arquivos em execução durante inicialização do sistema
- **Proteção em tempo real** - Proteção em tempo real do sistema de arquivos
- **Rastreamento do computador** - Rastreamento sob demanda do computador.

Os parâmetros do ThreatSense são especificamente otimizados para cada módulo e a modificação deles pode influenciar significativamente o funcionamento do sistema. Por exemplo, a alteração das configurações para sempre rastrear empacotadores em tempo real ou a ativação da heurística avançada no módulo de proteção em tempo real de sistema de arquivos podem resultar em um sistema mais lento. Portanto, recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Rastrear o computador.

7.1.5.1 Objetos

A seção **Objetos** permite definir quais arquivos serão rastreados quanto a infiltrações.

- **Links simbólicos** - (Apenas Rastreamento do computador) rastreia arquivos que contêm uma string de texto que é interpretada como um caminho para um arquivo ou diretório.
- **Arquivos de email** - (não disponível na Proteção em tempo real) rastreia arquivos de email.
- **Caixas de correio** - (não disponível na Proteção em tempo real) rastreia as caixas de correio do usuário no sistema. A utilização incorreta dessa opção pode resultar em um conflito com o seu cliente de e-mail. Para saber mais sobre as vantagens e desvantagens dessa opção, leia o seguinte artigo da base de dados de conhecimento.
- **Arquivos compactados**- (não disponível na Proteção em tempo real) rastreia arquivos compactados (.rar, .zip, .arj, .tar etc.).
- **Arquivos compactados de auto-extração** - (não disponível na Proteção em tempo real) rastreia arquivos contidos em arquivos compactados de auto-extração.
- **Empacotadores em tempo real** - ao contrário dos arquivos compactados padrão, os empacotadores em tempo real fazem a descompactação na memória. Quando essa opção está selecionada, empacotadores estáticos padrão (por exemplo UPX, yoda, ASPack, FGS) também são rastreados.

7.1.5.2 Opções

Na seção **Opções**, você pode selecionar os métodos utilizados durante um rastreamento do sistema. As opções disponíveis são:

- **Heurística** - A heurística utiliza um algoritmo que analisa a atividade (maliciosa) de programas. A principal vantagem da detecção heurística é a capacidade de detectar novos softwares maliciosos, que não existiam antes ou não estavam incluídos na lista de vírus conhecidos (banco de dados de assinatura de vírus).
- **Heurística avançada** - A heurística avançada é constituída por um algoritmo heurístico exclusivo, desenvolvido pela ESET, otimizado para a detecção de worms e cavalos de troia de computador escritos em linguagens de programação de alto nível. A capacidade de detecção do programa é significativamente maior por causa da heurística avançada.

7.1.5.3 Limpeza

Configurações de limpeza determinam a maneira pela qual o rastreamento limpa os arquivos infectados. Há três níveis de limpeza:

- **Sem limpeza** - Arquivos infectados não são limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que você escolha uma ação.
- **Limpeza padrão** - O programa tentará limpar ou excluir automaticamente um arquivo infectado. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá uma escolha de ações a serem seguidas. A escolha de ações de acompanhamento também será exibida se uma ação predefinida não puder ser concluída.
- **Limpeza rígida** - O programa limpará ou excluirá todos os arquivos infectados (inclusive arquivos compactados). As únicas exceções são os arquivos do sistema. Se não for possível limpar um arquivo, você receberá uma notificação e será solicitado a selecionar o tipo de ação a ser realizada.

Aviso: No modo padrão Limpeza padrão, arquivo compactados inteiros são excluídos somente se todos os arquivos do arquivo compactado estiverem infectados. Se um arquivo contém arquivos legítimos além dos arquivos infectados, eles não serão excluídos. Se um arquivo infectado for detectado no modo Limpeza rígida, todo o arquivo será excluído mesmo se houver arquivos limpos.

7.1.5.4 Exclusões

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Esta seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem excluídos do rastreamento.

Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento. Com os botões + e −, você pode ativar ou proibir o rastreamento de extensões de arquivos específicas.

A exclusão de arquivos do rastreamento será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa. Por exemplo, pode ser aconselhável excluir arquivos *log*, *cfg* e *tmp*. O formato correto para digitar as extensões de arquivo é:
log
cfg
tmp

7.1.5.5 Limites

A seção **Limites** permite especificar o tamanho máximo de objetos e nível de compactação de arquivos compactados a serem rastreados:

- **Tamanho máximo:** Define o tamanho máximo dos objetos que serão rastreados. O módulo antivírus só vai rastrear objetos menores do que o tamanho especificado. Não recomendamos alterar o valor padrão, pois geralmente não há razão para modificá-lo. Essa opção deverá ser alterada apenas por usuários avançados que tenham razões específicas para excluir objetos maiores do rastreamento.
- **Tempo máximo do rastreamento:** Define o valor de tempo máximo para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento.
- **Nível de compactação de arquivos:** Especifica a profundidade máxima do rastreamento de arquivos compactados. Não recomendamos alterar o valor padrão de 10; sob circunstâncias normais, não haverá razão para modificá-lo. Se o rastreamento for encerrado prematuramente devido ao número de arquivos compactados aninhados, o arquivo compactado permanecerá desmarcado.
- **Tamanho máximo do arquivo:** Essa opção permite especificar o tamanho máximo dos arquivos contidos em arquivos compactados (quando são extraídos) a serem rastreados. Se o rastreamento for encerrado prematuramente por causa desse limite, o arquivo compactado permanecerá sem verificação.

7.1.5.6 Outros

Ativar otimização inteligente

Com a Otimização inteligente ativada, as configurações são otimizadas para garantir o nível mais eficiente de rastreamento, sem comprometer a velocidade de rastreamento. Os diversos módulos de proteção fazem rastreamento de maneira inteligente, utilizando diferentes métodos de rastreamento. Otimização inteligente não é definida rigidamente no produto. A Equipe de Desenvolvimento ESET está continuamente implementando novas mudanças que são integradas no ESET Endpoint Antivirus através de atualizações regulares. Se a Otimização inteligente estiver desativada, somente as configurações definidas pelo usuário no núcleo do ThreatSense do módulo particular serão aplicadas durante a realização de um rastreamento.

Rastrear fluxos dados alternativos (apenas rastreamento sob demanda)
Fluxos de dados alternativos (bifurcações de recursos/dados) usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

7.1.6 Uma infiltração foi detectada

As infiltrações podem atingir o sistema a partir de vários pontos de entrada: páginas da Web, pastas compartilhadas, email ou dispositivos de computador removíveis (USB, discos externos, CDs, DVDs, etc.).

Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, etc., recomendamos que você faça o seguinte:

1. Clique em **Rastrear o computador**.
2. Clique em **Rastreamento inteligente** (para obter mais informações, consulte a seção Rastreamento inteligente 14).
3. Após o rastreamento ter terminado, revise o relatório para obter informações como o número dos arquivos verificados, infectados e limpos.

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a malware.

Como exemplo geral de como as infiltrações são tratadas no ESET Endpoint Antivirus, suponha que uma infiltração seja detectada pelo monitor do sistema de arquivos em tempo real, usando o nível de limpeza padrão. A proteção em tempo real tentará limpar ou excluir o arquivo. Se não houver uma ação predefinida disponível para o módulo de proteção em tempo real, você será solicitado a selecionar uma opção em uma janela de alertas. Geralmente as opções **Limpar**, **Excluir** e **Nenhuma ação** estão disponíveis. Não é recomendado selecionar **Nenhuma ação**, uma vez que o(s) arquivo(s) infectado(s) é(são) deixado(s) em seu estado infectado. Esta opção é feita para situações quando você tem certeza de que o arquivo é inofensivo e foi detectado por engano.

Limpeza e exclusão - Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou um código malicioso a esse arquivo. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo ao seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Exclusão de arquivos em arquivos compactados - No modo de limpeza padrão, os arquivos compactados serão excluídos por inteiro somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Tenha cautela ao executar um rastreamento com **Limpeza rígida**, com esse tipo de limpeza o arquivo compactado será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

7.2 Proteção à web e email

Para acessar a Proteção à web e emails, no menu principal clique em **Configuração** > **Web e email**. A partir daqui, você pode acessar mais configurações detalhadas para cada módulo clicando em **Configuração**.

Proteção do acesso à Web - monitora a comunicação HTTP/HTTPS entre os navegadores da Internet e os servidores remotos.

Proteção do cliente de email - fornece controle da comunicação por email recebida através dos protocolos POP3 e IMAP.

Proteção antiphishing - bloqueia os potenciais ataques de phishing que vêm de sites ou domínios listados no banco de dados de malware da ESET.

7.2.1 Proteção do acesso à Web

A proteção do acesso à Web monitora a comunicação entre os navegadores da Internet e os servidores remotos para conformidade com regras de HTTP (Protocolo de Transferência de Hipertexto) ou HTTPS.

7.2.1.1 Portas

Na guia **Portas** você pode definir os números das portas utilizadas para a comunicação HTTP. Por padrão, os números de portas 80, 8080 e 3128 estão predefinidos.

7.2.1.2 Modo ativo

o ESET Endpoint Antivirus também contém o submenu **Modo Ativo**, que define o modo de verificação para os navegadores da web. O Modo ativo examina os dados transferidos de aplicativos acessando a Internet, independentemente de eles serem marcados como navegadores da web. Se não estiver ativado, a comunicação dos aplicativos é monitorada gradualmente em lotes. Isso diminui a eficiência do processo de verificação dos dados, mas também aumena a compatibilidade para os aplicativos listados. Se nenhum problema ocorrer ao usá-lo, recomendamos que você ative a verificação ativa marcando a caixa de seleção ao lado do aplicativo desejado.

Quando um aplicativo com acesso à rede fizer download de dados, eles são primeiro salvos em um arquivo temporário criado pelo ESET Endpoint Antivirus. Nesse momento, os dados não estão disponíveis para o aplicativo determinado. Assim que o download for concluído, ele será rastreado contra códigos maliciosos. Se não for encontrada infiltração, os dados serão enviados para o aplicativo original. Esse processo fornece controle completo das comunicações feitas por um aplicativo controlado. Se o modo passivo estiver ativado, os dados serão destinados ao aplicativo original para evitar atingir o tempo limite.

7.2.1.3 Listas de URL

A seção **Listas de URL** permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação. Os sites na lista de endereços bloqueados não serão acessíveis. Os sites na lista de endereços excluídos são acessados sem serem rastreados quanto a código malicioso.

Para permitir apenas o acesso a URLs listados na lista de **URL permitido**, selecione **Restringir endereços URL**.

Para ativar uma lista, selecione **Ativado** ao lado do nome da lista. Se você desejar ser notificado ao inserir um endereço da lista atual, selecione **Notificado**.

Os símbolos especiais *(asterisco) e ?(ponto de interrogação) podem ser usados ao construir listar de URL. O asterisco substitui qualquer string de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista.

7.2.2 Proteção de email

A proteção de email fornece controle da comunicação por email recebida pelos protocolos POP3 e IMAP. Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado inclusos no mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com a base de dados de assinaturas de vírus. O rastreamento das comunicações por protocolos POP3 e IMAP é independente do cliente de email usado.

Mecanismo ThreatSense - a configuração avançada do rastreamento de vírus permite configurar destinos de rastreamento, métodos de detecção, etc. Clique em **Configuração** para exibir a janela de configuração do scanner de vírus detalhada.

Depois que um email tiver sido rastreado, uma notificação com o resultado do rastreamento pode ser anexada à mensagem. Você pode selecionar **Anexar mensagens de marca ao assunto do email**. Não se deve confiar nas mensagens de marca sem questioná-las, pois elas podem ser omitidas em mensagens HTML problemáticas e podem ser forjadas por alguns vírus. As opções disponíveis são:

Nunca - nenhuma mensagem de marca será adicionada,
Somente para email infectado - Somente mensagens contendo software malicioso serão marcadas como rastreadas,
Para todos os emails rastreados - o programa anexará mensagens a todos os emails rastreados.

Modelo adicionado ao assunto de email infectado - edite esse modelo para modificar o formato de prefixo do assunto de um email infectado.

Acrescentar mensagem de marca ao rodapé de email - Marque essa caixa de seleção se você quiser que a proteção de email inclua um alerta de vírus em um email infectado. Esse recurso permite a filtragem simples de emails infectados. Esse recurso aumenta o nível de credibilidade para os destinatários e, se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do email ou do remetente.

7.2.2.1 Verificação de protocolo POP3

O protocolo POP3 é o protocolo mais amplamente utilizado para receber comunicação em um aplicativo cliente de email. O ESET Endpoint Antivirus fornece proteção a esse protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Certifique-se de que o modulo está ativado para que a filtragem de protocolo funcione corretamente, a verificação do protocolo POP3 é feita automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os números das portas devem ser delimitados por vírgula.

Se a opção **Ativar verificação de protocolo POP3** estiver selecionada, todo o tráfego POP3 é monitorado em busca de software malicioso.

7.2.2.2 Verificação de protocolo IMAP

O IMAP (Internet Message Access Protocol) é outro protocolo de Internet para recuperação de emails. O IMAP tem algumas vantagens sobre o POP3, por exemplo, vários clientes podem se conectar simultaneamente à mesma caixa de correio e gerenciar informações de estado das mensagens, tais como se a mensagem foi ou não lida, respondida ou excluída. O ESET Endpoint Antivirus fornece proteção para este protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Certifique-se de que a verificação de protocolo IMAP está ativada para que o módulo funcione corretamente, o controle do protocolo IMAP é feito automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 143 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os números das portas devem ser delimitados por vírgula.

Se a opção **Ativar verificação de protocolo IMAP** estiver selecionada, todo o tráfego IMAP é monitorado em busca de software malicioso.

7.3 Antiphishing

O termo *roubo de identidade* define uma atividade criminal que usa engenharia social (a manipulação de usuários para obter informações confidenciais). O roubo de identidade é frequentemente usado para obter acesso a dados sensíveis como números de contas bancárias, números de cartão de crédito, códigos de PIN ou nomes de usuário e senhas.

Recomendamos manter o Antiphishing ativado (**Configuração** > **Entrar nas preferências do aplicativo ...** > **Proteção antiphishing**). Todos os potenciais ataques de phishing que vêm de sites ou domínios listados no banco de dados de malware da ESET serão bloqueados e uma notificação de alerta será exibida informando sobre o ataque.

8. Controle de dispositivo

O ESET Endpoint Antiviruspermite rastrear, bloquear ou ajustar filtros e/ou permissões estendidos e define a capacidade de um usuário de acessar e trabalhar com um determinado dispositivo. Isso é útil se a intenção do administrador do computador for evitar o uso de dispositivos com conteúdo não solicitado pelos usuários.

Dispositivos externos compatíveis:

- Armazenamento em disco (HDD, unidade USB)
- CD/DVD
- Impressora USB
- Dispositivo de criação de imagem
- Porta serial
- Rede
- Dispositivo portátil

Se um dispositivo bloqueado por uma regra existente for inserido, uma janela de notificação será exibida e o acesso ao dispositivo não será concedido.

O relatório de controle de dispositivos registra todas as ocorrências que acionam o controle de dispositivos. As entradas de relatórios podem ser visualizadas a partir da janela principal do programa do ESET Endpoint Antivirus em **Ferramentas** > **Relatórios** 21.

8.1 Editor de regras

As opções de configuração do controle de dispositivos podem ser modificadas em **Configuração** > **Acessar preferências do aplicativo**. > **Controle de dispositivos**.

Clicar em **Ativar controle do dispositivo** ativa o recurso de controle de dispositivos no ESET Endpoint Antivirus. Assim que o Controle de dispositivo estiver ativado, você pode gerenciar e editar funções de controle de dispositivos. Selecione a caixa de seleção ao lado de um nome de regra para ativar ou desativar a regra.

Use os botões + ou − para adicionar ou remover regras. As regras são listadas por ordem de prioridade, com regras de prioridade superior mais próximas do início. Para reorganizar a ordem, arraste e solte uma regra para sua nova posição ou clique em ⚙ e escolha uma das opções.

ESET Endpoint Antivirus detecta automaticamente todos os dispositivos atualmente inseridos e seus parâmetros (tipo de dispositivo, fabricante, modelo, número de série). Em vez de criar regras manualmente, clique na opção **Preencher**, selecione o dispositivo e clique em **Continuar** para criar a regra.

Determinados dispositivos podem ser permitidos ou bloqueados de acordo com seu usuário, grupo de usuários ou com base em vários parâmetros adicionais que podem ser especificados na configuração da regra. A lista de regras contém diversas descrições de uma regra, como nome, tipo de dispositivo, gravidade do relatório e ação a ser realizada após conectar um dispositivo ao seu computador.

Nome

Insira uma descrição da regra no campo **Nome** para melhor identificação. A caixa de seleção **Regra ativada** ativa ou desativa esta regra. Isso pode ser útil caso não deseje excluir a regra permanentemente.

Tipo de dispositivo

Escolha o tipo de dispositivo externo do menu suspenso. As informações sobre o tipo de dispositivo são coletadas do sistema operacional. Os dispositivos de armazenamento incluem discos externos ou leitores de cartão de memória convencionais conectados via USB ou FireWire. Leitores de cartões inteligentes diz respeito a dispositivos que leem qualquer mídia com um circuito integrado incorporado, por exemplo cartões SIM ou cartões de autenticação. Scanners e câmeras são exemplos de dispositivos de imagens. Como esses dispositivos oferecem apenas informações sobre suas ações e não oferecem informações sobre os usuários, eles só podem ser bloqueados de forma global.

Ação

O acesso a dispositivos que não sejam de armazenamento pode ser permitido ou bloqueado. Por outro lado, as regras de dispositivos de armazenamento permitem a seleção de uma das seguintes configurações de direitos:
Ler/Gravar - Será permitido acesso total ao dispositivo
Apenas leitura - Será permitido acesso apenas para leitura ao dispositivo
Bloquear - O acesso ao dispositivo será bloqueado

Tipo de critério

Selecione **Grupo do dispositivo** ou **Dispositivo**. Outros parâmetros mostrados a seguir podem ser usados para ajustar as regras e adequá-las a dispositivos.
Fabricante - Filtragem por nome ou ID do fabricante
Modelo - O nome específico do dispositivo
Número de série - Os dispositivos externos geralmente têm seus próprios números de série. No caso de CD/DVD, este é o número de série da mídia em si, e não o da unidade de CD/DVD

OBSERVAÇÃO: Se esses parâmetros não estiverem definidos, a regra irá ignorar estes campos enquanto faz a correspondência. Os parâmetros de filtragem em todos os campos de texto não fazem diferenciação de maiúsculas e minúsculas; caracteres curinga (*, ?) não são aceitos.

DICA: Para ver informações sobre um dispositivo, crie uma regra para o tipo de dispositivos e conecte o dispositivo ao seu computador. Assim que o dispositivo tiver sido conectado, detalhes do dispositivo serão exibidos no Relatório de controle do dispositivo 21.

Gravidade do registro em relatório

Sempre - criar relatório de todos os eventos
Diagnóstico - Registra informações necessárias para ajustar o programa
Informações - registra as mensagens informativas, e também todos os registros mencionados anteriormente
Aviso - Registra mensagens de erros críticos e de aviso
Nenhum - Nenhum registro será feito

Lista de usuários

As regras podem ser limitadas a determinados usuários ou grupos de usuários adicionando-os à Lista de usuários:
Editar... - Abre o **Editor de identidade** onde você pode selecionar usuários ou grupos. Para definir uma lista de usuários, selecione-os na lista **Usuários** no lado esquerdo e clique em **Adicionar**. Para remover um usuário, selecione o nome na lista de **Usuários selecionados** e clique em **Remover**. Para mostrar todos os usuários do sistema, selecione **Mostrar todos os usuários**. Se a lista estiver vazia, todos os usuários terão permissão

OBSERVAÇÃO: Nem todos os dispositivos podem ser filtrados por regras do usuário (por exemplo, dispositivos de criação de imagem não fornecem informações sobre usuários, apenas sobre ações).

9. Ferramentas

O menu **Ferramentas** inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados.

9.1 Relatórios

Os relatórios contêm informações sobre todos os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detectadas. O registro em relatório atua como uma ferramenta essencial na análise do sistema, na detecção de ameaças e na solução de problemas. O registro em relatório realiza-se ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento de relatórios. É possível visualizar mensagens de texto e relatórios diretamente do ambiente do ESET Endpoint Antivirus, bem como arquivar relatórios.

Os relatórios podem ser acessados no menu principal do ESET Endpoint Antivirus clicando em **Ferramentas** > **Relatórios**. Selecione o tipo de relatório desejado, utilizando o menu suspenso **Relatório** na parte superior da janela. Os seguintes relatórios estão disponíveis:

1. **Ameaças detectadas** - Informações sobre eventos relacionados à detecção de infiltrações.
2. **Eventos** - Todas as ações importantes executadas pelo ESET Endpoint Antivirus são registradas nos Relatórios de eventos.
3. **Rastrear o computador** - os resultados de todos os rastreamentos concluídos são exibidos nessa janela. Clique duas vezes em qualquer entrada para exibir os detalhes de um rastreamento de computador específico.
4. **Controle de dispositivos** - Contém registros de dispositivos ou mídias removíveis que foram conectados ao computador. Apenas dispositivos com uma regra de controle de dispositivo serão registrados no relatório. Se a regra não coincidir com um dispositivo conectado, uma entrada de relatório para um dispositivo conectado não será criada. Aqui você também pode visualizar detalhes, como tipo de dispositivo, número de série, nome do fornecedor e tamanho da mídia (se disponível).
5. **Sites filtrados** - Esta lista é útil se você quiser visualizar uma lista de sites que foram bloqueados pela Proteção do acesso à web 18. Nesses relatórios você poderá ver o horário, URL, status, endereço IP, usuário e aplicativo que criaram uma conexão para o site específico.

Clique com o botão direito do mouse em qualquer relatório e clique em **Copiar** para copiar o conteúdo desse relatório para a área de transferência.

9.1.1 Manutenção dos relatórios

A configuração de relatórios do ESET Endpoint Antivirus pode ser acessada na janela principal do programa. Clique em **Configuração** > **Entrar nas preferências do aplicativo...** > **Ferramentas** > **Relatórios** . Você pode especificar as seguintes opções para relatórios:

- **Excluir relatórios antigos automaticamente** - as entradas de relatórios anteriores ao número de dias especificado são automaticamente excluídas.
- **Otimizar relatórios automaticamente** - ativa a desfragmentação automática de relatórios se a porcentagem especificada de relatórios não utilizados foi excedida.

Todas as informações relevantes apresentadas na interface gráfica do usuário, mensagens de ameaça e de eventos podem ser armazenados em formatos de texto legíveis como texto simples ou CSV (valores separados por vírgula). Se quiser tornar esses arquivos disponíveis para processamento usando ferramentas de terceiros, marque a caixa de seleção ao lado de **Ativar o registro de arquivos de texto**.

Para definir a pasta de destino para a qual os relatórios serão salvos, clique em **Configuração** ao lado de **Configuração avançada**.

Com base nas opções selecionadas em **Arquivos de texto de relatórios: Editar** é possível salvar os relatórios com as seguintes informações escritas:

- Eventos como *Nome de usuário e senha inválidos*, *Banco de dados de assinatura de vírus não pode ser atualizado* etc., são gravados no arquivo *eventslog.txt*.
- Ameaças detectadas pelo Scanner na inicialização, Proteção em tempo real ou Rastrear o computador são armazenadas no arquivo chamado *threatslog.txt*.
- Os resultados de todos os rastreamentos concluídos são salvos no formato *scanlog.NUMBER.txt*.
- Dispositivos bloqueados pelo controle de dispositivos são monitorados no devctllog.txt

Para configurar os filtros para os **Registros de relatório padrão de rastreamento do computador**, clique em **Editar** e selecione/desselecione tipos de relatório conforme necessário. Uma explicação mais profunda para esses tipos de relatórios pode ser encontrada e, Filtragem de relatórios 22.

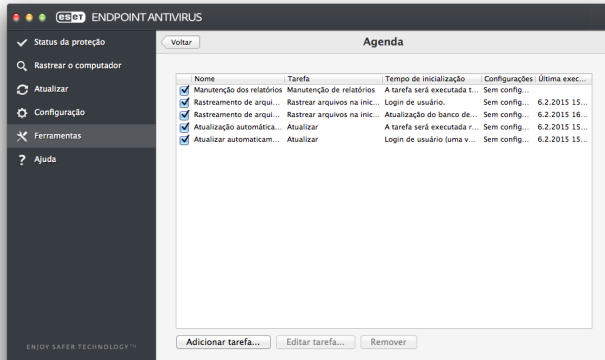
9.1.2 Filtragem de relatórios

Registra em relatório as informações de armazenamento sobre eventos importantes do sistema. O recurso de filtragem de relatório permite exibir registros sobre um evento específico.

Os tipos de relatórios utilizados com mais frequência são listados a seguir:

- **Avisos críticos** - erros críticos do sistema (por exemplo, falha ao iniciar a proteção antivírus)
- **Erro** - Erros como " *Erro ao fazer download de arquivo* " e erros críticos
- **Avisos** - mensagens de aviso
- **Registros informativos** - mensagens informativas, incluindo atualizações bem-sucedidas, alertas, etc.
- **Registros de diagnóstico** - informações necessárias para ajustar o programa e também todos os registros descritos acima.

9.2 Agenda

A **Agenda** pode ser encontrada no menu principal do ESET Endpoint Antivirus em **Ferramentas**. A **Agenda** contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e o horário, bem como os perfis especificados para serem utilizados durante a execução da tarefa.

Por padrão, as seguintes tarefas agendadas são exibidas na Agenda:

- Manutenção de relatórios (depois de ativar **Mostrar tarefas do sistema** na configuração da agenda)
- Rastreamento de arquivos durante inicialização do sistema após logon do usuário
- Rastreamento de arquivos durante inicialização do sistema após atualização bem sucedida do banco de dados de assinatura de vírus
- Atualização automática regular
- Atualizar automaticamente após logon do usuário

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique segurando a tecla CTRL na tarefa que deseja modificar e clique em **Editar** ou selecione a tarefa e clique em **Editar tarefa**.

9.2.1 Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique em **Adicionar tarefa** ou clique com segurando a tecla CTRL e selecione **Adicionar** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo**
- **Atualizar**
- **Manutenção dos relatórios**
- **Rastreamento sob demanda do computador**
- **Rastrear arquivos na inicialização do sistema**

OBSERVAÇÃO: Ao escolher **Executar aplicativo**, você pode executar programas como um usuário do sistema chamado de "ninguém". As permissões para executar aplicativos através da Agenda são definidas pelo Mac OS X.

No exemplo abaixo, usaremos a Agenda para adicionar uma nova tarefa de atualização, já que atualizar é uma das tarefas agendadas usadas com mais frequência:

1. Selecione **Atualizar** no menu suspenso **Tarefa agendada**.
2. Digite um nome para a tarefa no campo **Nome da tarefa**.
3. Selecione a frequência da tarefa no menu suspenso **Executar tarefa**. Com base na frequência selecionada, diferentes parâmetros de atualização serão exibidos para sua especificação. Se selecionar **Definida pelo usuário**, você será solicitado a especificar uma data/hora no formato *cron* (consulte a seção Criar regra definida pelo usuário 24 para obter mais detalhes).
4. Na próxima etapa, defina a ação a ser tomada se a tarefa não puder ser executada ou concluída na hora agendada.
5. Clique em **Terminar**. A nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

Por padrão, o ESET Endpoint Antivirus contém as tarefas agendadas pré-definidas para garantir a funcionalidade correta do produto. Elas não devem ser alteradas e ficam ocultas, por padrão. Para tornar essas tarefas visíveis, no menu principal clique em **Configuração** > **Entrar nas preferências do aplicativo** > **Agenda** e selecione **Exibir tarefas do sistema**.

9.2.2 Criação de uma tarefa definida pelo usuário

Existem alguns parâmetros especiais que devem ser definidos ao selecionar Definido pelo usuário como o tipo de tarefa no menu suspenso Executar tarefa.

A data e hora de uma tarefa **Definida pelo usuário** deve ser inserida no formato cron prorrogado para ano (uma string de 6 caracteres incluindo campos separados por espaços em branco):

```
minuto(0-59) hora(0-23) dia do mês(1-31) mês(1-12) ano(1970-2099) dia da semana(0-7)(Domingo = 0 ou 7)
```

Por exemplo:

```
30 6 22 3 2012 4
```

Os seguintes caracteres especiais são suportados em expressões cron:

- asterisco (`*`) - a expressão irá corresponder para todos os valores no campo; por exemplo, um asterisco no terceiro campo (dia do mês) significa todo dia
- hífen (`-`) - define intervalos; por exemplo `3-9`
- vírgula (`,`) - separa os itens de uma lista; por exemplo `1,3,7,8`
- barra (`/`) - define incrementos de intervalos; por exemplo `3-28/5` no terceiro campo (dia do mês) significa o 3.º dia do mês e a cada 5 dias.

Os nomes dos dias (Monday-Sunday) e dos meses (January-December) não são suportados.

OBSERVAÇÃO: Se você definir tanto um dia do mês quanto um dia da semana, o comando será executado apenas quando ambos os campos forem iguais.

9.3 Live Grid

O Live Grid Early Warning System mantém a ESET, imediatamente e continuamente, informada sobre novas infiltrações. O sistema de alerta bidirecional do Live Grid Early Warning System tem uma única finalidade: melhorar a proteção que podemos proporcionar-lhe. A melhor maneira de garantir que vemos novas ameaças assim que elas aparecem é fazermos "link" com o máximo possível de nossos clientes e usar as informações coletadas para manter nossas informações de assinatura de vírus constantemente atualizadas. Selecione uma das duas opções para o Live Grid:

1. Você pode escolher não ativar o Live Grid Early Warning System. Você não perderá nenhuma funcionalidade do software, mas, em alguns casos, o ESET Endpoint Antivirus poderá responder mais rápido a novas ameaças do que a atualização do banco de dados de assinatura de vírus.
2. É possível configurar o Live Grid Early Warning System para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido. Essa informação pode ser enviada para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar seu banco de dados de ameaças e melhorar nossa capacidades de detecção de ameaças.

O Live Grid Early Warning System coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Enquanto há uma possibilidade de que isso possa ocasionalmente revelar algumas informações sobre você ou seu computador (usuários em um caminho de diretório, etc.) para o Laboratório de ameaças da ESET, essas informações não serão utilizadas para QUALQUER outra finalidade que não seja nos ajudar a reagir imediatamente contra novas ameaças.

Para acessar a configuração do Live Grid a partir do menu principal, clique em **Configuração** > **Entrar nas preferências do aplicativo** > **Live Grid**. Selecione **Ativar o sistema de reputação do ESET Live Grid (recomendado)**para ativar o Live Grid e clique em **Configuração** ao lado de **Opções avançadas**.

9.3.1 Arquivos suspeitos

Por padrão, o ESET Endpoint Antivirus é configurado para enviar arquivos suspeitos ao Laboratório de ameaças da ESET para análise detalhada. Se você não quer enviar esses arquivos automaticamente, desmarque **Envio de arquivos suspeitos** (**Configuração** > **Entrar nas preferências do aplicativo** > **Live Grid** > **Configuração**).

Se encontrar um arquivo suspeito, você poderá enviá-lo ao nosso Laboratório de ameaças para análise. Para fazer isso, clique em **Ferramentas** > **Enviar arquivo para análise** na janela principal do programa. Se for um aplicativo malicioso, sua assinatura será adicionada à próxima atualização do banco de dados de assinaturas de vírus.

Envio de informações estatísticas anônimas - o ESET Live Grid Early Warning System coleta informações anônimas sobre seu computador relacionadas a ameaças detectadas recentemente. Essas informações incluem o nome da ameaça, a data e o horário em que ela foi detectada, a versão do produto de segurança da ESET, a versão do seu sistema operacional e a configuração de local. Essas estatísticas são normalmente enviadas aos servidores da ESET, uma ou duas vezes por dia.

A seguir há um exemplo de um pacote estatístico enviado:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/
rdgFR1463[1].zip
```

Filtro de exclusões - Esta opção permite excluir determinados tipos de arquivos do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, .rtf, etc.). Você pode adicionar os tipos de arquivos à lista de arquivos excluídos.

Email de contato (opcional) - seu endereço de email será utilizado se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

9.4 Quarentena

O principal objetivo da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Endpoint Antivirus.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo rastreador de antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de ameaças da ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão de ser colocado na quarentena (por exemplo, objeto adicionado pelo usuário) e o número de ameaças. A pasta de quarentena (*/Library/ Application Support/Eset/esets/cache/quarantine*) permanece no sistema, mesmo após a desinstalação do ESET Endpoint Antivirus. Os arquivos em quarentena são armazenados em um formato criptografado e seguro e podem ser restaurados novamente após a instalação do ESET Endpoint Antivirus.

9.4.1 Colocação de arquivos em quarentena

o ESET Endpoint Antivirus coloca automaticamente os arquivos excluídos em quarentena (se você não desativou essa opção na janela de alertas). A partir da janela de quarentena, você pode clicar em Quarentena para adicionar manualmente qualquer arquivo na quarentena. Também é possível clicar pressionando o ctrl em um arquivo com o a qualquer momento e selecionar Serviços > ESET Endpoint Antivirus - Adicionar arquivos para quarentena no menu de contexto para enviar o arquivo para a quarentena.

9.4.2 Restaurar um arquivo da quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original, para isso selecione um arquivo na quarentena e clique em **Restaurar**. Restaurar também está disponível no menu de contexto, clique segurando a tecla CTRL em um determinado arquivo na janela de Quarentena e clique em **Restaurar**. É possível usar **Restaurar para** para restaurar um arquivo para um local diferente do local original do qual ele foi colocado em quarentena.

9.4.3 Envio de um arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi avaliado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de ameças da ESET. Para enviar um arquivo diretamente da quarentena, clique segurando a tecla CTRL nele e selecione **Enviar arquivo para análise** no menu de contexto.

9.5 Privilégios

as configurações do ESET Endpoint Antivirus podem ser muito importantes para a política de segurança da organização. Modificações não autorizadas podem pôr em risco a estabilidade e a proteção do seu sistema. Consequentemente, você pode escolher quais usuários terão permissão para editar a configuração do programa.

Você pode configurar usuários privilegiados sob **Configuração** > **Entrar nas preferências do aplicativo** > **Usuário** > **Privilégios**.

Para fornecer segurança máxima ao seu sistema, é fundamental que o programa seja configurado corretamente. Modificações não autorizadas podem resultar na perda de dados importantes. Para definir uma lista de usuários privilegiados, selecione-os na lista **Usuários** no lado esquerdo e clique em **Adicionar**. Para remover um usuário, selecione o nome na lista de **Usuários Privilegiados** no lado direito e clique em **Remover**. Para mostrar todos os usuários do sistema, selecione **Mostrar todos os usuários**.

OBSERVAÇÃO: Se a lista de usuários privilegiados estiver vazia, todos os usuários do sistema terão permissão para editar as configurações do programa.

9.6 Modo de apresentação

Modo de apresentação é um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Ele também pode ser utilizado durante apresentações que não podem ser interrompidas pela atividade do antivírus. Quando ativado, todas as janelas pop-up são desativadas e tarefas agendadas não são executadas. A proteção do sistema ainda é executada em segundo plano, mas não requer interação com nenhum usuário.

Para ativar o Modo de apresentação manualmente, clique em **Configuração** > **Entrar nas preferências do aplicativo...** > **Modo de apresentação** > **Ativar o modo de apresentação**.

Marque a caixa de seleção ao lado de **Ativar automaticamente o modo de apresentação em tela cheia** para acionar o Modo de apresentação automaticamente quando os aplicativos forem executados no modo de tela cheia. Quando este recurso está ativado, o modo de apresentação será iniciado sempre que você iniciar um aplicativo em tela cheia e será interrompido automaticamente ao sair do aplicativo. Isso recurso é especialmente útil para iniciar uma apresentação.

Você também pode selecionar **Desativar o modo de apresentação automaticamente após** para definir o período de tempo em minutos após o qual o modo de apresentação será desativado automaticamente.

Ativar automaticamente o modo de apresentação é um risco de segurança em potencial, pois o ícone do status de proteção ESET Endpoint Antivirus ficará laranja e exibirá um aviso.

9.7 Processos em execução

A lista de **Processos em execução** exibe os processos em execução no seu computador. O ESET Endpoint Antivirus oferece informações detalhadas sobre os processos em execução para proteger os usuários com a tecnologia ESET Live Grid.

- **Processo** - nome do processo que está atualmente em execução em seu computador. Também é possível usar o Monitor de Atividade (localizado em */Applications/Utilities*) para visualizar todos os processos em execução no computador.
- **Nível de risco** - Na maioria dos casos, o ESET Endpoint Antivirus e a tecnologia do ESET Live Grid atribuem níveis de risco aos objetos (arquivos, processos, etc.), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, os objetos recebem um nível de risco. Os aplicativos conhecidos marcados em verde estão definitivamente limpos (na lista de permissões) e serão excluídos do rastreamento. Isso melhora a velocidade tanto do rastreamento sob demanda quanto do rastreamento em tempo real. Quando um aplicativo é marcado como desconhecido (em amarelo), ele não é necessariamente software mal-intencionado. Geralmente, é apenas um aplicativo mais recente. Se não tiver certeza sobre o arquivo, você poderá enviá-lo para o Laboratório de Ameaça ESET para anállise. Se for detectado que o arquivo é um aplicativo malicioso, sua assinatura será adicionada em uma das atualizações posteriores.
- **Número de usuários** - O número de usuários que utilizam um determinado aplicativo. Essas informações são coletadas pela tecnologia ESET Live Grid.
- **Hora da descoberta** - Período de tempo a partir do momento em que o aplicativo foi detectado pela tecnologia do ESET Live Grid.
- **ID do pacote do aplicativo** - nome de processo do aplicativo ou do fornecedor.

Ao clicar em determinado processo, as seguintes informações serão exibidas na parte inferior da janela:

- **Arquivo** - local de um aplicativo no computador
- **Tamanho do arquivo** - tamanho físico do arquivo no disco
- **Descrição de arquivo** - características do arquivo com base na descrição do sistema operacional
- **ID do pacote do aplicativo** - nome de processo do aplicativo ou do fornecedor
- **Versão do arquivo** - informações do editor do aplicativo
- **Nome do produto** - nome do aplicativo e/ou nome comercial

10. Interface do usuário

As opções de configuração da interface do usuário permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções podem ser acessadas no menu principal clicando em **Configuração** > **Entrar nas preferências do aplicativo** > **Interface**.

- Para exibir a tela inicial do ESET Endpoint Antivirus na inicialização do sistema, selecione **Mostrar tela inicial na inicialização**.
- A opção **Aplicativo presente no Dock** permite que você exiba o ícone ESET Endpoint Antivirus no Mac OS Dock e alterne entre o ESET Endpoint Antivirus e outros aplicativos em execução pressionando *cmd-tab*. As alterações serão implementadas depois que você reiniciar o ESET Endpoint Antivirus (geralmente acionado pela reinicialização do computador).
- **Usar menu padrão** permite que você use certos atalhos de teclado (consulte Atalhos de teclado 10) e ver os itens de menu padrão (Interface de usuário, Configuração e Ferramentas) na barra de menus do Mac OS (parte superior da tela).
- Ativar **Mostrar dicas de ferramentas** para exibir dicas de ferramenta quando o cursor é colocado sobre certas opções no ESET Endpoint Antivirus.
- **Mostrar arquivos ocultos** permite que você veja e selecione arquivos ocultos na configuração de **Destinos de rastreamento** para um **Rastreamento do computador**.

10.1 Alertas e notificações

A seção **Alertas e notificações** permite que você configure como os alertas de ameaças e as notificações do sistema são tratados no ESET Endpoint Antivirus.

Desativar a opção **Exibir alertas** desativará todas as janelas de alerta e é adequado apenas em situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

Selecionar **Exibir notificações na área de trabalho** criará janelas de alerta que não exigem interação do usuário exibidas na área de trabalho (no canto superior direito da tela, por padrão). Você pode definir o período no qual a notificação será exibida, ajustando o valor de **Fechar notificações automaticamente depois de** X **segundos**.

10.1.1 Configuração avançada de alertas e notificações

O ESET Endpoint Antivirus exibe janelas de diálogo de alerta informando sobre novas versões do programa, atualizações do sistema operacional, desativação de certos componentes do programa, exclusão dos relatórios, etc. Você pode suprimir cada notificação individualmente selecionando **Não mostrar este diálogo novamente**.

Lista de caixas de diálogos (**Configuração** > **Entrar nas preferências do aplicativo...** > **Alertas e notificações** > **Configuração**) exibe a lista de todos os diálogos de alerta acionados pelo ESET Endpoint Antivirus. Para ativar ou reprimir cada notificação, marque a caixa de seleção à esquerda do **Nome da caixa de diálogo**. Além disso, você pode definir as **Condições de exibição** de acordo com as quais as notificações sobre novas versões de programas e atualizações do sistema operacional serão exibidas.

10.2 Menu de contexto

Para disponibilizar recursos do ESET Endpoint Antivirus a partir do menu de contexto, clique em **Configuração** > **Entrar nas preferências do aplicativo** > **Menu de contexto** e marque a caixa de seleção ao lado de **Integrar no menu de contexto**. Alterações serão implementadas depois de sair ou reiniciar seu computador. Opções do menu de contexto estarão disponíveis na área de trabalho e na janela **Finder** quando você clicar segurando a tecla CTRL em qualquer arquivo ou pasta.

11. Atualizar

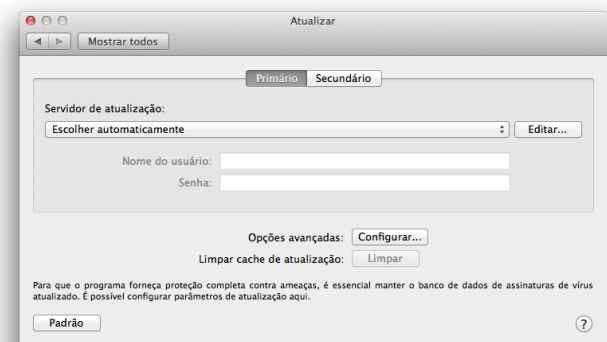
Atualizar o ESET Endpoint Antivirus com regularidade é necessário para manter o nível máximo de segurança. O módulo de atualização garante que o programa esteja sempre atualizado por meio de download do banco de dados de assinatura de vírus mais recente.

Clique em **Atualizar** no menu principal oara ver seu status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida, e se uma atualização será necessária. Para iniciar o processo de atualização manualmente, clique em **Atualizar banco de dados de assinatura de vírus**.

Em circunstâncias normais, quando o download das atualizações é feito adequadamente, a mensagem *A atualização não é necessária - O banco de dados de assinatura de vírus está atualizado* aparecerá na janela Atualizar se você tiver o banco de dados de assinatura de vírus mais recente. Se o banco de dados de assinatura de vírus não puder ser atualizados, recomendamos verificar as configurações de atualização 28 - a razão mais comum para esse erro é a inserção de dados de licença 9 incorretos ou definições incorretas das configurações de conexão 31.

A janela **Atualizar** também contém informações sobre a versão do banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET, onde todas as assinaturas adicionadas em determinada atualização são exibidas.

11.1 Configuração da atualização

A seção de configuração da atualização especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação para esses servidores. Por padrão, o menu suspenso **Servidor de atualização** está configurado para **Escolher automaticamente**, a fim de garantir que os arquivos de atualização sejam obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede.

A lista de servidores de atualização disponíveis pode ser acessada por meio do menu suspenso **Servidor de atualização**. Para adicionar um novo servidor de atualização, clique em **Editar**, digite o endereço do novo servidor no campo de entrada **Servidor de Atualização** e clique em **Adicionar**.

o ESET Endpoint Antivirus permite definir um servidor de atualização alternativo ou de failover. Seu servidor **Primário** poderia ser o seu servidor imagem e o servidor **Secundário** poderia ser o servidor de atualização ESET padrão. O servidor secundário deve diferir do primário, caso contrário ele não será usado. Se você não especificar um servidor secundário de atualização, Nome de usuário e Senha, a funcionalidade de atualização de failover não funcionará. Também é possível selecionar Escolher automaticamente para e digitar seu Nome de usuário e Senha nos campos apropriados para que o ESET Endpoint Antivirus selecione automaticamente o melhor servidor de atualização a ser usado.

Se você está tendo dificuldade ao tentar fazer download das atualizações do banco de dados de assinatura de vírus, clique em **Limpar Cache de Atualização** para excluir os arquivos de atualização temporários.

11.1.1 Configuração avançada

Para desativar notificações exibidas depois de cada atualização bem-sucedida, selecione **Não exibir notificação sobre atualização bem-sucedida**.

Ativar Atualizações pré-lançamento para fazer download dos módulos de desenvolvimento que estão terminando os testes finais. Atualizações pré-lançamento muitas vezes contêm correções para problemas de produtos. A atualização atrasada atualiza algumas horas depois de ser liberada, para garantir que seus clientes não receberão atualizações até que elas estejam confirmadas como livres de quaisquer problemas no estado natural.

O ESET Endpoint Antivirus registra instantâneos de módulos do programa e banco de dados de assinatura de vírus para uso com o recurso de **Atualização de rollback**. Deixe **Criar instantâneos dos arquivos de atualização** ativado para que o ESET Endpoint Antivirus registre esses instantâneos automaticamente. Caso suspeite que uma nova atualização do banco de dados de vírus e/ou módulos do programa esteja instável ou corrompida, será possível reverter para a versão anterior e desativar atualizações por um período de tempo definido. Alternativamente, será possível ativar atualizações desativadas anteriormente caso tenha as adiado indefinidamente. Quando reverter para uma atualização anterior, use o menu suspenso Definir período suspenso para especificar o período de tempo para o qual você deseja suspender as atualizações. Se você selecionar até a revogação as atualizações normais não serão retomadas até que você restaure as atualizações manualmente. Tenha cuidado ao selecionar essa configuração.

Definir a idade máxima do banco de dados automaticamente - Permite definir o tempo máximo (em dias) depois do qual o banco de dados de assinatura de vírus será relatado como desatualizado. O valor padrão é 7 dias.

11.2 Como criar tarefas de atualização

Clique em Atualizar > **Atualização do banco de dados da assinatura de vírus** para acionar manualmente uma atualização de banco de dados de assinatura de vírus.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas estão ativadas no ESET Endpoint Antivirus:

- **Atualização automática regular**
- **Atualizar automaticamente após logon do usuário**

Cada uma das tarefas de atualização pode ser modificada para atender às suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte Agenda 23.

11.3 Atualização para uma nova compilação

Para obter a máxima proteção, é importante usar a compilação mais recente do ESET Endpoint Antivirus. Para verificar se há uma nova versão, clique em **Início** no menu principal à esquerda. Uma notificação será exibida no canto inferior da tela quando uma nova versão estiver disponível. Clique em **Saiba mais** para exibir uma nova janela que contém o número da versão da nova compilação e o registro de alterações.

Clique em **Download** para fazer download da compilação mais recente. Clique em **Fechar** para fechar a janela e fazer download da atualização mais tarde.

Se você clicou em **Sim**, o arquivo será obtido por download para a sua pasta de downloads (ou para a pasta padrão definida pelo navegador). Quando o download do arquivo estiver concluído, inicie o arquivo e siga as instruções de instalação. Suas informações de licença serão automaticamente transferidas para a nova instalação.

Recomendamos que você verifique se há atualizações regularmente, especialmente durante a instalação do ESET Endpoint Antivirus usando CD/DVD.

11.4 Atualizações do sistema

O recurso de atualizações do sistema Mac OS X é um componente importante para a proteção de usuários contra software malicioso. Para ter o máximo de seguranla, recomendamos instalar essas atualizações assim que forem disponibilizadas. O ESET Endpoint Antivirus o notificará sobre as atualizações ausentes de acordo com o nível de importância. Você pode ajustar o nível de atualização importância para o qual as notificações são exibidas em **Configuração** > **Entrar nas preferências do aplicativo** > **Alertas e notificações > Configuração** utilizando o menu suspenso de **Condições de exibição** ao lado de **Atualizações do sistema operacional**.

- **Mostrar todas as atualizações** - exibirá uma notificação sempre que uma atualização do sistema estiver faltando
- **Mostrar apenas recomendados** - somente as atualizações recomendadas serão notificadas

Se não quiser ser notificado sobre atualizações faltando, desmarque a caixa ao lado de **Atualizações do sistema operacional**.

A janela de notificação fornece uma visão geral das atualizações disponíveis para o sistema operacional OS X e os aplicativos atualizados através da ferramenta nativa do OS X - Atualizações de software. Você pode executar a atualização diretamente a partir da janela de notificação ou na seção **Início** do ESET Endpoint Antivirus clicando em **Instalar a atualização faltando**.

A janela de notificação contém o nome do aplicativo, versão, tamanho, propriedades (bandeiras) e qualquer informação adicional sobre atualizações disponíveis. A coluna **Bandeiras** contém as seguintes informações:

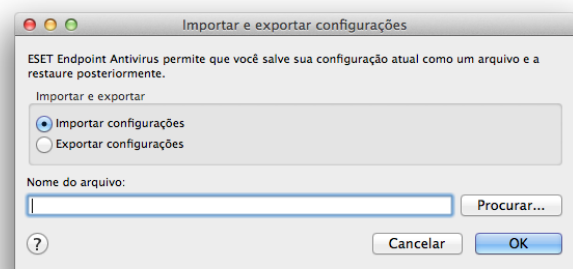
- **[recomendado]** - o fabricante do sistema operacional recomenda que você instale esta atualização para aumentar a segurança e estabilidade do sistema
- **[reiniciar]** - é necessário reiniciar o computador depois da instalação
- **[desligar]** - é necessário desligar e ligar novamente o computador depois da instalação

A janela de notificações exibe as atualizações recuperadas pela ferramenta de linha de comando chamada ‘softwareupdate’. Atualizações recuperadas por esta ferramenta podem variar das atualizações exibidas pelo aplicativo ‘Atualizações de software’. Se desejar instalar todas as atualizações disponíveis exibidas na janela ‘Atualizações do sistema faltando’ e também aquelas exibidas pelo aplicativo ‘Atualizações de software’, é preciso usar a ferramenta de linha de comando ‘softwareupdate’. Para saber mais sobre esta ferramenta, leia o manual 'softwareupdate' digitando `man softwareupdate` em uma janela no **Terminal**. Isto é recomendado apenas para usuários avançados.

12. Diversos

12.1 Importar e exportar configurações

Para importar uma configuração existente ou exportar suas configurações ESET Endpoint Antivirus, clique em **Configuração** > **Importar e exportar configurações**.

A importação e a exportação é útel caso precise fazer backup da configuração atual do ESET Endpoint Antivirus para que ela possa ser utilizada posteriormente. A exportação de configurações também é conveniente para os usuários que desejam utilizar suas configurações preferenciais ESET Endpoint Antivirus em diversos sistemas. Os usuários podem importar facilmente um arquivo de configuração para transferir suas configurações desejadas.

12.1.1 Importar configurações

Para importar uma configuração, clique em **Configuração** > **Importar e exportar configurações** no menu principal e selecione **Importar configurações**. Clique em **Navegar** para ir ao arquivo de configuração que você deseja importar.

12.1.2 Exportar configurações

Para exportar uma configuração, clique em **Configuração** > **Importar e exportar configurações** no menu principal e selecione **Exportar configurações**. Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.

12.2 Configuração do servidor proxy

Para configurar as configurações do servidor Proxy, clique em **Configuração** > **Entrar nas preferências do aplicativo** > **Servidor Proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todas as funções do ESET Endpoint Antivirus. Os parâmetros definidos aqui serão utilizados por todos os módulos que exigem conexão com a Internet. O ESET Endpoint Antivirus é compatível com autenticação Basic Access e NTLM (NT LAN Manager).

Para especificar as configurações do servidor proxy para esse nível, selecione **Usar servidor proxy** e insira o endereço IP ou URL do servidor proxy no campo **Servidor proxy**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão).

Se a comunicação com o servidor proxy exigir autenticação, digite um **Nome de usuário** e uma **Senha** válidos nos respectivos campos.

12.3 Cache local compartilhado

Para ativar o uso do Cache local compartilhado, clique em Configuração> Entrar nas preferências do aplicativo > Cache local compartilhado e marque a caixa de seleção ao lado de Ativar armazenamento em cache utilizando o Cache local compartilhado da ESET. O uso deste recurso melhorará o desempenho em ambientes virtualizados ao eliminar o rastreamento duplicado na rede. Isso garante que cada arquivo seja rastreado somente uma vez e armazenado no cache compartilhado. Quando ativada, as informações sobre rastreamentos de arquivos e pastas são salvas em sua rede no cache local. Se você realizar um novo rastreamento, o ESET Endpoint Antivirus verificará se há arquivos rastreados no cache. Se os arquivos corresponderem, eles serão excluídos do rastreamento.

As configurações do Cache local compartilhado contém o seguinte:

- **Endereço do servidor** - Nome ou endereço IP do computador no qual o cache está localizado
- **Porta** - número da porta usada para a comunicação (3537 por padrão)
- **Senha** - Senha do cache local compartilhado (opcional)

OBSERVAÇÃO: Para obter instruções detalhadas sobre como instalar e configurar o Cache local compartilhado da ESET, consulte o Guia do Usuário de Cache local compartilhado da ESET. (O guia está disponível apenas em inglês.)